REMARKS/ARGUMENTS

Claims 1-22 remain in this application. Applicants request reconsideration of this application in view of these remarks and arguments.

Objections

The Examiner has objected to Applicants' amendment filed March 13, 2006 under 35 U.S.C. 132(a) stating that it introduces new matter based on amendments made to Claim 1. More particularly, the Examiner first states that the limitations "a first encryption key *associated* with traffic encryption for group communications" are not supported by the original disclosure. In support of this conclusion, the Examiner states "Paragraph [0045] states that the GCK, which is the first encryption key is 'never used for the actual encryption of traffic as it is considered a long term key'".

Applicants disagree with the Examiner's reasoning. The language that the Examiner quotes from Claim 1 does not state that the first encryption key is used for the actual encryption of traffic. It states that the first encryption key is "*associated*" with traffic encryption for group communications because a modified version of this key or in other words a derivative of the first encryption is used for traffic encryption for group communications. Thus, the support for this language in Claim 1 cited by the Examiner is found elsewhere in the same paragraph [0045], which states "[i]ndirectly, the Group Cipher Key (GCK) is used to encrypt outbound talkgroup calls. . . [T]he modified group cipher key (MGCK), which is a derivative of the GCK, is directly used for traffic encryption". This is an example of how the first encryption key is associated with traffic encryption for group communications.

The Examiner further argues that the limitations recited in Claim 1 of forwarding the key "to a second system device other than a mobile station" is not supported by the original disclosure. In support of this conclusion, that Examiner states "[p]aragraph [0026] discusses the KMF generating the GCK for distribution in the system. A mobile station is considered part of the system, and nowhere in the disclosure is such a negative limitation

found that explicitly states the exclusion of a mobile station from being the second device. Furthermore, the Examiner asserts that the action of forwarding to a second device doesn't necessarily demand the second device be the next 'hop' in the system". Applicants again disagree with the Examiner's reasoning.

First of all, Applicants do not understand why the Examiner makes the assertion that the action of forwarding to a second device doesn't necessarily demand that the second device be the next hop in the system. Applicants certainly agree that the language of Claim 1 is not limited to the second system device being the next hop to the first system device. Moreover, Applicants agree that the specification in general discloses that the GCK is forwarded to a mobile station (see FIG. 16 and paragraphs [0106] to [0108]). However, Applicants did not want Claim 1 to read on the GCK being forwarded to a mobile station. FIG. 15 and paragraphs [0102] to [0103] disclose that the GCK (for example) is also forwarded to a system device that is other than a mobile station (e.g., the ZC), and Applicants limited the language of Claim 1 to include only the case where the second system device was other than a mobile station so as to particularly point out and distinctly claim the invention. Thus, the language "other than a mobile station" is meant to make clear the boundaries of the subject matter for which protection is sought. M.P.E.P. §2173.01 states "Applicant may use functional language, alternative expressions, *negative limitations*, or any style of expression or format of claim which makes clear the boundaries of the subject matter for which protection is sought".

Finally, the Examiner argues that the limitations recited in Claim 1 of "forwarding the second encryption key to a third system device other than a mobile station" is not supported by the original disclosure. In support of this conclusion, that Examiner states "[p]aragraph [0071] discloses that the second key is stored at the MS (mobile station), thus it is necessary for this key to have been forwarded to the mobile station". Applicants disagree with the Examiner's reasoning.

First, the language of Claim 1 cited by the Examiner finds support in FIG. 15 and paragraphs [0103] and [0105]. Where the second key is, for instance, the MGCK, this key

is forwarded to a third system device, e.g., a BS (base station). In addition and contrary to what the Examiner assumes, it is not necessary that the MGCK was forwarded to the MS. The specification discloses how the MGCK can be independently generated in the MS because the MS has the first encryption key, e.g., GCK, (see FIG. 16 and paragraphs [0106] to [0108]) and the third encryption key, e.g., CCK, (see FIG. 14 and paragraph [0095]) that are combined to generate the second encryption key, e.g., MGCK. In fact, it is this faulty assumption (i.e., that the ultimate destination of the MGCK is the MS) that is the basis of the Examiner's rejection of the claims.

The Examiner states that the same arguments apply to the similar amendments to Claims 2, 10 and 11 in regards to the limitation precluding the forwarding to a device other than a mobile station. Likewise, Applicants arguments with respect to the Examiner's objections to Claim 1 apply to the Examiner's objections to Claims 2, 10 and 11. Based on their arguments, Applicants request that the Examiner remove the objections to Claims 1, 2, 10 and 11 based on 35 U.S.C. 132(a).

Claim Rejections – 35 USC §112

The Examiner has rejected Claims 1, 2, 10 and 11 under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement because the claims contain subject matter that was not described in the specification in a way to reasonably convey to one skilled in the art that the inventor(s), at the time the application was filed, had possession of the claimed invention based on the discussion of new matter in the Office Action. Based on Applicants' argument above addressing the Examiner's new matter objections, Applicants request that the Examiner remove these §112 first paragraph rejections to Claims 1, 2, 10 and 11.

The Examiner has rejected Claims 1 and 32 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention stating that the limitation of the first encryption key being "associated" with traffic encryption is unclear. M.P.E.P. §2173.02 states that the "examiner's focus during Examination of claims for compliance with

definiteness of 35 U.S.C. 112, second paragraph, is whether the claim meets the threshold requirements of clarity and precision, not whether more suitable language . . . [is] available. . . [A] reasonable degree of particularity and distinctness [is the threshold]. . . Definiteness of claim language must be analyzed, not in a vacuum, but it light of (among other factors): . . . [t]he content of the particular application disclosure". M.P.E.P. §2173.05(a) further states that the "meaning of every term used in a claim should be apparent from the prior art or from the specification and drawings at the time the application is filed".

When the term "associated" is analyzed in view of language in the specification, the meaning of the term is apparent and meets the threshold requirement of clarity and precision. For example, take the paragraph [0045] in the specification that the Examiner refers to. In the context of this paragraph the language in Claims 1 and 2 of "the first encryption key. . . associated with traffic encryption for group communications" has a *reasonable degree* of particularity and distinctness. It is apparent from paragraph [0045] that a first encryption key (e.g., GCK) is associated with traffic encryption for group communications by being "*[i]ndirectly used* to encrypt outbound talkgroup calls". It is further apparent from language in this paragraph that the language "associated with" excludes the first encryption key being directly used for traffic encryption for group communications. Therefore, Applicants request that the Examiner remove the §112, second paragraph, rejections of Claims 1 and 2.

Claim Rejections – 35 USC §103

The Examiner has rejected Claims 1-4, 6-8, 10-18 and 21 under 35 U.S.C. 103(a) as being unpatentable over Roelofson, and in further view of Tiedemann (USPN 6381454). Applicants traverse these rejections. To establish a *prima facie* case of obviousness, and hence to find Claims 1-4, 6-8, 10-18 and 21 unpatentable under 35 U.S.C. § 103(a) over the combination of Roelofson and Tiedemann, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success.

Finally, the prior art reference (or references when combined) must teach or suggest all of the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not be based upon applicant's disclosure. MPEP at § 2142.

In the present case, all three criteria are not met because the combined teachings of Roelofson and Tiedemann, et al. references do not teach or suggest all of the claim limitations of independent Claims 1 and 2. More particularly, Claims 1 and 2 recite the limitations of "generating, *by the second system device*, a second encryption key associated with traffic encryption for group communications by combining the first encryption key with a third encryption key; and forwarding the second encryption key to a third system device other than a mobile station and other than the first and second system devices", which are not taught or suggested in either the Roelofson or Tiedemann references.

The Examiner conceded that Roelofson fails to disclose "storing the first encryption key at the second system device, and forwarding the second encryption key to a third system device other than a mobile station and other than the first and second system devices". Moreover, Applicants further submit that Roelofson fails to disclose the second system device (which is other than a mobile station) generating the second encryption key by combining the first and third encryption keys. At most, Roelofson implies that the second encryption key (e.g., MGCK) is generated in the mobile station, since the mobile station is forwarded both the first (e.g., GCK) and third (e.g., CCK) encryption keys that are used to generate the second encryption key. Tiedemann also does not disclose the second encryption key (associated with traffic encryption for group communications) being generated in a second system device by combining the first encryption key and the third encryption key. Tiedemann (for instance in the language on page 14, lines 42-50 cited by the Examiner and in FIG. 8) merely discloses two parameters, a SMEKEY and VPMASK that are sent to a mobile station via an HLR (e.g., second system device) and a VLR (e.g., third system device) from an AC (e.g., first system device). However, as is clearly shown

there is no encryption key that is generated in the HLR by combining two other keys. The two parameters referred to in the language cited by the Examiner originate in the AC.

Therefore, since limitation are missing from the combined teachings of Roelofson and Tiedemann, the Examiner should remove the 103(a) rejections of Claims 1-4, 6-8, 10-18 and 21,

The Examiner has further rejected: Claims 5 under 35 U.S.C. 103(a) as being unpatentable over Roelofson in view of Tiedemann and further in view of Jackson (USPN 6477387); Claims 9 and 22 under 35 U.S.C. 103(a) as being unpatentable over Roelofson in view of Tiedemann and further in view of Roelofson ("Security Issues for TETRA Networks"); and Claims 19 and 20 under 35 U.S.C. 103(a) as being unpatentable over Roelofson in view of Tiedemann and further in view of Marshall (USPN 4888800). Applicants traverse these rejections. As argued above, the combined teachings of Roelofson and Tiedemann fail to disclose the limitations of "generating, by the second system device, a second encryption key associated with traffic encryption for group communications by combining the first encryption key with a third encryption key; and forwarding the second encryption key to a third system device other than a mobile station and other than the first and second system devices". Applicants further submit that the Jackson, Marshall and other Roelofson references also fail to teach or disclose these limitations.

Therefore, Applicants further request that the Examiner remove the 103(a) rejections with respect to Claims 5, 9, 19-20 and 22.

No amendment made was related to the statutory requirements of patentability unless expressly stated herein. No amendment made was for the purpose of narrowing the scope of any claim, unless Applicant has argued herein that such amendment was made to distinguish over a particular reference or combination of references.

The Applicants believe that the subject application, as amended, is in condition for allowance. Such action is earnestly solicited by the Applicants.

In the event that the Examiner deems the present application non-allowable, it is requested that the Examiner telephone the Applicant's attorney at the number indicated below so that the prosecution of the present case may be advanced by the clarification of any continuing rejection.

Please charge any fees that may be due to Deposit Account 502117, Motorola, Inc.

Respectfully submitted,

SEND CORRESPONDENCE TO:

By: /Valerie M. Davis/

Motorola, Inc.
1303 East Algonquin Road
IL01/3rd Floor
Schaumburg, IL 60196
Customer Number: 22917

Valerie M. Davis
Attorney of Record
Reg. No.: 50,203

Telephone:847-576-6733
Fax No.: 847-576-0721
Email: vdavis@motorola.com